SAGRADO
Universidad del Sagrado Corazón

Política para el Uso de las Redes de Conexión

Efectivo: 2019.07.01

Propósito

Esta Política define los estándares para conectar computadoras, servidores u otros dispositivos a la red de Sagrado (también conocido como "Universidad"). Los estándares están diseñados para minimizar el riesgo de daños potenciales, incluidos los financieros, la pérdida de trabajo y la pérdida de datos que podrían producirse en computadoras y servidores que no están configurados o mantenidos adecuadamente; y para garantizar que los dispositivos conectados a la red no estén tomando medidas que pudiera afectar negativamente el rendimiento de la red.

Sagrado proporciona una red segura para nuestras necesidades y servicios educativos, de investigación, de instrucción y administrativos. El acceso de una computadora que no está protegida a la red de la Universidad hace la red vulnerable a ataques y virus que comprometen los servicios estudiantiles, las computadoras y la integridad de la red. Los daños de estos atentados podrían incluir la pérdida de datos sensitivos y confidenciales, la interrupción de los servicios de red y el daño a los sistemas internos críticos de la Universidad. Las universidades que han experimentado atentados serios también han sufrido daños a su imagen pública. Los usuarios que conectan computadoras, servidores y otros dispositivos a la red de la Universidad deben seguir estándares específicos y tomar medidas específicas.

Aplicabilidad

Esta Política es aplicable a todos los estudiantes, profesores y personal de Sagrado, y cualquier otro que utilice la red de la Universidad (“usuarios”).

Conexión Apropiada

Los usuarios pueden conectar dispositivos a la red del campus en puntos de conectividad apropiados incluyendo conectores de voz y/o datos, a través de un punto de acceso de red

inalámbrico aprobado, a través de un túnel VPN o SSH o a través de mecanismos de acceso remoto como DSL, cable módems y módems tradicionales usando líneas telefónicas. Las modificaciones o extensiones a la red con frecuencia pueden causar efectos no deseados, incluida la pérdida de conectividad. Estos efectos no siempre son inmediatos, ni siempre se encuentran en el sitio de las modificaciones. Como resultado, la extensión o modificación de la red de Sagrado debe realizarse dentro de las directrices publicadas de la Oficina de Información y Tecnología Integrada ("ITI"); El Principal Oficial de Información ("CIO") puede hacer excepciones para el personal aprobado en unidades de trabajo que puedan demostrar competencia en el manejo del hardware.

Registros en la Red

Es posible que se les requiera a los usuarios de la red de Sagrado certifiquen su información al conectar un dispositivo. Los usuarios también pueden necesitar instalar un agente autorizado en sus computadoras antes de que puedan conectarse a la red. El uso de dicho agente sería auditar la computadora para verificar el cumplimiento de los estándares de seguridad definidos a continuación.

ITI mantiene una base de datos que identifica la computadora como máquina única, además de la dirección de red e información del propietario con el objetivo de contactar al propietario de una computadora cuando sea necesario. ITI puede contactar al propietario registrado de una computadora cuando su computadora se ha visto comprometida y está lanzando un ataque de denegación de servicio o si se ha emitido un aviso de violación de derechos de autor para la dirección de IP utilizada por esa persona.

Estándares de Seguridad

Estos estándares de seguridad se aplican a todos los dispositivos que se conectan a la red de Sagrado a través de puertos estandarizados de la Universidad, a través de servicios inalámbricos o cualquier recurso disponible, local o remoto a través de conexiones dentro y fuera del campus de la Universidad.

Los dueños de las computadoras que se van a conectar a la Red son responsables de lo siguiente:

- Deben asegurarse de que sus computadoras y otros dispositivos que utilicen sean capaces de ejecutar software antivirus/*antimalware* y que tengan instalado y en funcionamiento el software antivirus con licencia de la Universidad u otros productos apropiados de protección contra virus.

- Deben actualizar los archivos de definición al menos una vez por semana.

- Deben instalar los parches de seguridad más recientes en el sistema tan pronto como sea práctico o según lo indique ITI. Cuando las máquinas no se pueden reparar, es posible que se requieran otras acciones para asegurar la máquina de manera adecuada.

- Deben aplicar protecciones adicionales para las computadoras que contienen Información Restringida o Confidencial, tal como se define en la Política de Seguridad de la Información y según determine ITI.

Servicios de la Red Proporcionados por la Universidad

ITI es responsable de proporcionar servicios de red confiables para todo el recinto universitario. Como tal, los usuarios o las unidades de trabajo o departamentos no pueden ejecutar ningún servicio o sistema que no esté expresamente autorizado por ITI.

Protección de la Red

- ITI utiliza varios métodos para proteger la red de Sagrado, tales como: monitorear intrusos externos, analizar anfitriones (*hosts*) en la red en busca de anomalías sospechosas y bloquear el tráfico o movimiento de data dañino.

- Todo el tráfico de red entrante y saliente a través de la red de Sagrado es monitoreado por un sistema de detección de intrusos en busca de signos de actividades sospechosas o de posibles ataques. Al conectar una computadora o dispositivo a la red, los usuarios reconocen que el tráfico de red hacia y desde su computadora puede ser escaneado.

- ITI escanea rutinariamente la red, buscando vulnerabilidades. A veces, puede ser necesario realizar pruebas más exhaustivas para detectar y confirmar la existencia de vulnerabilidades. Al conectarse a la red, los usuarios aceptan que su computadora o dispositivo sea escaneado en busca de posibles vulnerabilidades.

- ITI se reserva el derecho de tomar las medidas necesarias para limitar las exposiciones de seguridad a la Universidad o incluyendo el tráfico incorrecto de la red.

- ITI se reserva el derecho de limitar ciertos tipos de tráfico que entran a la red de Sagrado que se sabe que causa daños a la red o los *hosts* en ella.

- ITI puede controlar otros tipos de tráfico que consumen demasiada capacidad de red, como el tráfico de intercambio de archivos.

Estándares mínimos para controles de red

El CIO es responsable de que el acceso a la red tenga como mínimo los siguientes estándares de control:

- El sistema debe estar en una red protegida por *firewall* y que se comparta solamente con sistemas en el mismo dominio de seguridad.
- Todo el tránsito de Información Restringida a través de la red debe estar encriptado.
- No se permitirá la transmisión de contraseñas sin cifrar.
- El acceso a la red estará restringido al mínimo necesario para realizar las funciones requeridas.

Informar el Uso Indebido del Uso de las Redes de Conexión

Los usuarios tienen la responsabilidad de reportar sospechas de un uso indebido de las redes de conexión incluyendo, pero sin limitarse a, sospechas de actividades ilícitas o impropias al Principal Oficial de Información al 787.728.1515, ext. 3571, o por correo electrónico a luis.gotelli@sagrado.edu.

Inspección y monitoreo la información y los recursos de tecnología e información ("IT"). pueden ser necesarios para cumplir con esta Política, realizar investigaciones o auditorías, garantizar la seguridad de una persona o de la Universidad, cumplir con la ley o garantizar el funcionamiento adecuado de los recursos de IT. Solo el CIO (o designado) puede autorizar esta inspección y monitoreo.

Se espera que los usuarios de los recursos de IT cooperen con cualquier investigación de abuso de Políticas. La falta de cooperación puede ser motivo de cancelación de privilegios de acceso u otras medidas disciplinarias.

Consultas sobre esta Política

Las consultas sobre el alcance y la interpretación y las de esta Política deben dirigirse al Principal Oficial de Información al 787.728.1515, ext. 3571, o por correo electrónico a luis.gotelli@sagrado.edu.

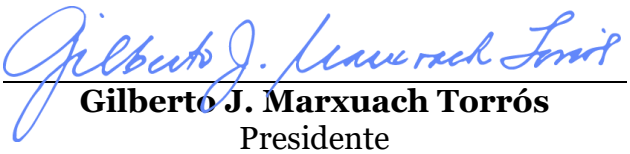
Denuncias de Violaciones a la Política

Las violaciones a esta Política deben dirigirse al Asesor Jurídico al 787.728.1515, ext. 1221, o por correo electrónico a cameliac.fernandez@sagrado.edu, o al Oficial de Cumplimiento e Integridad.

Violaciones a esta Política

La Universidad del Sagrado Corazón se reserva el derecho de interpretar esta Política en su administración, implementación y aplicación. Cualquier violación de esta Política por parte de un estudiante, profesorado o personal o cualquier otra persona puede resultar en una acción disciplinaria que puede incluir la expulsión de la Universidad (estudiantes) o la terminación de la relación laboral (personal docente y administrativo) u otras acciones legales apropiadas.

Si existe alguna ambigüedad en cualquier disposición de esta Política, la Universidad se reserva la discreción de interpretarla de acuerdo con el propósito para el cual fue establecida, el impacto en las operaciones de la Universidad y la buena fe, a menos que cualquier ley establezca lo contrario.



Gilberto J. Marxuach Torrós
Presidente